login screen that can be used in accordance with the preferred embodiment. Figures 2B-D illustrate login screens that can be used in accordance with alternative embodiments.--

In the Claims:

Please cancel Claims 1-27 without prejudice and add the following new claims:

28. A method of authenticating a user, the method comprising:

associating the user with a personal communication device possessed by the user;

generating a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting a password associated with the user to be the new password;

transmitting the token to the personal communication device; and

receiving the password from the user.

29. The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

30. The method of Claim 28, further comprising receiving a request from the user for the token.

31. The method of Claim 30, wherein the request is transmitted by the user through the personal communication device.

32. The method of Claim 28, wherein the personal communication device is a mobile phone.

33. The method of Claim 28, wherein the personal communication device is a pager.

34. A user authentication system comprising:

a user database configured to associate a user with a personal communication device possessed by the user;

a control module configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;

a communication module configured to transmit the token to the personal communication device; and

an authentication module configured to receive the password from the user.

35. The system of Claim 34, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.

36. The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

37. A method of regulating access to a secure system, the method comprising:

associating the user with a personal communication device possessed by the user;

associating the user with an account, wherein an initiation of access through the account requires that the account be activated;

receiving a request transmitted by the personal communication device; and

in response to the receipt of the request, activating the account.

38. The method of Claim 37, further comprising deactivating the account within a predetermined amount of time after the account is activated.

39. The method of Claim 37, wherein an initiation of access through the account further requires that the user supply a valid password.

40. The method of Claim 39, further comprising:

generating a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting the valid password to be the new password;

transmitting the token to the personal communication device; and

receiving the valid password from the user.

41. The method of Claim 40, wherein the new password is generated by concatenating the token and the passcode.

42. The method of Claim 40, wherein the token is transmitted in response to the receipt of the request.

43. A method of regulating access to a secure system, the method comprising:

receiving a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user;

in response to the receipt of the request, transmitting the token to the personal communication device;

receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and

granting access to the secure system based at least upon the received login data.

44. The method of Claim 43, wherein the login data is additionally based upon a passcode known to the user.

45. The method of Claim 43, wherein the login data comprises a password.

46. The method of Claim 45, wherein the password comprises a passcode and the token, and wherein the passcode is known to the user.

47. The method of Claim 46, wherein the password is a concatenation of the passcode and the token.

48. The method of Claim 46, wherein the password is a hashed concatenation of the passcode and the token.

49. The method of Claim 43, further comprising generating the token.

50. An access control system comprising:

a communication module configured to receive a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request;

a user token server configured to generate a valid password based at least upon the token; and

an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.

51. The system of Claim 50, wherein the user token server is further configured to generate the valid password based additionally upon a passcode that is known to the user.

52. The system of Claim 51, wherein the valid password is a concatenation of the passcode and the token.

53. The system of Claim 50, wherein the user token server is further configured to generate the token.